ONTology

本体信任框架白皮书

Version 2.0.0

2019/07

摘要

长期以来，人们通过“技术”、“法制”、“社群”等不同维度和方法来建立信任，但这样多来源、多系统、多方法的单点式信任协作也带来了非常高的协作成本，阻碍了信任协作的深度和广度。虽然互联网技术日新月异，但关于信任的很多痛点至今依然存在，如信任源分散化、数据零散化、个体角色缺失、身份认证不准确、虚假信息难判断等。在社会治理、经济协作、金融服务等各种协作过程中，每天因“信任”产生着大量的成本。

去中心化、不可篡改的区块链从一定机制上建立起了特定场景下的技术信任，但要和现实世界的业务场景结合起来需要更多的融合机制，如何构造一个结合多样性信任和一体化应用的信任机制，成为对新一代“信任”基础体系的追求。

本体致力于建立一个体系化、流程化、一体化的信任生态，本体将作为信任生态体系的基础设施和连接器，为信任源的有效协同、为数据源的互联互通、为各类分布式应用服务提供完整的底层技术基础设施 [1]。

本书重点针对本体信任框架的组成模块进行阐述。

1. 本体是一个支持众多信任协作场景的基础性体系，根据场景和应用范围的应用会持续地进行各类模块与协议的扩展。本基础设施技术白皮书仅描述本体在当前阶段规划的基础架构和协议。

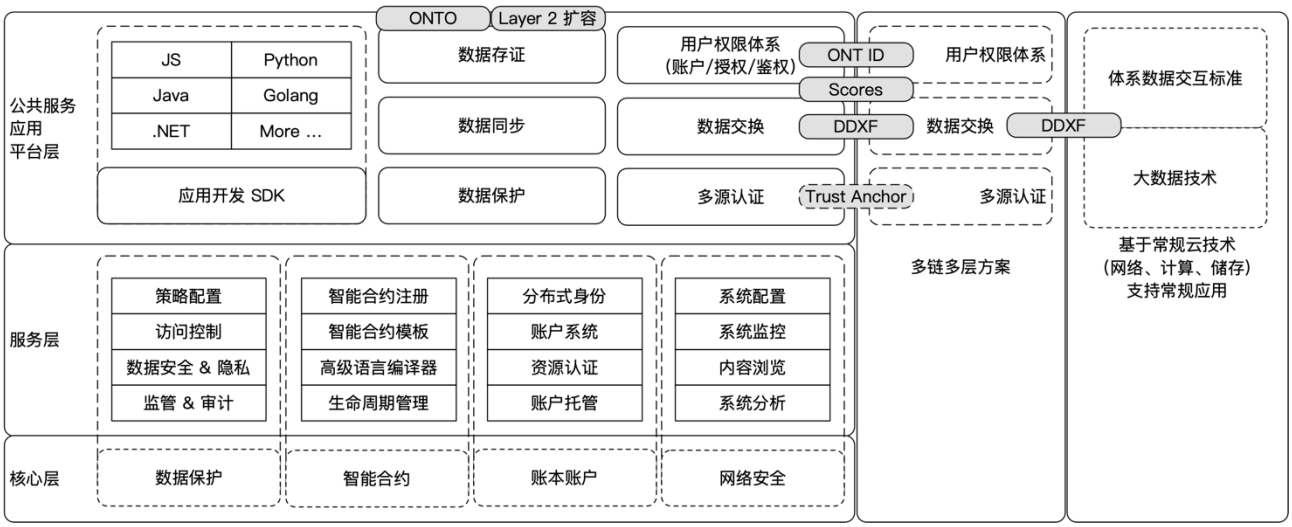
目录

1. 概述

本书是本体白皮书的一部分，描述本体信任框架，包含服务层工具、平台层应用模块，以及本体应用协议。

本体服务层。基于本体核心层提供模块化服务层工具，使得整个架构具备更好的伸缩性及灵活性；

本体应用层。本体应用层提供上层基于身份和数据资产的应用平台，给出通用信息资产化、资产交易的解决方案，打造本体公共服务平台。本体应用层支持跨链调用。应用层跨链支持异构链跨链方案。

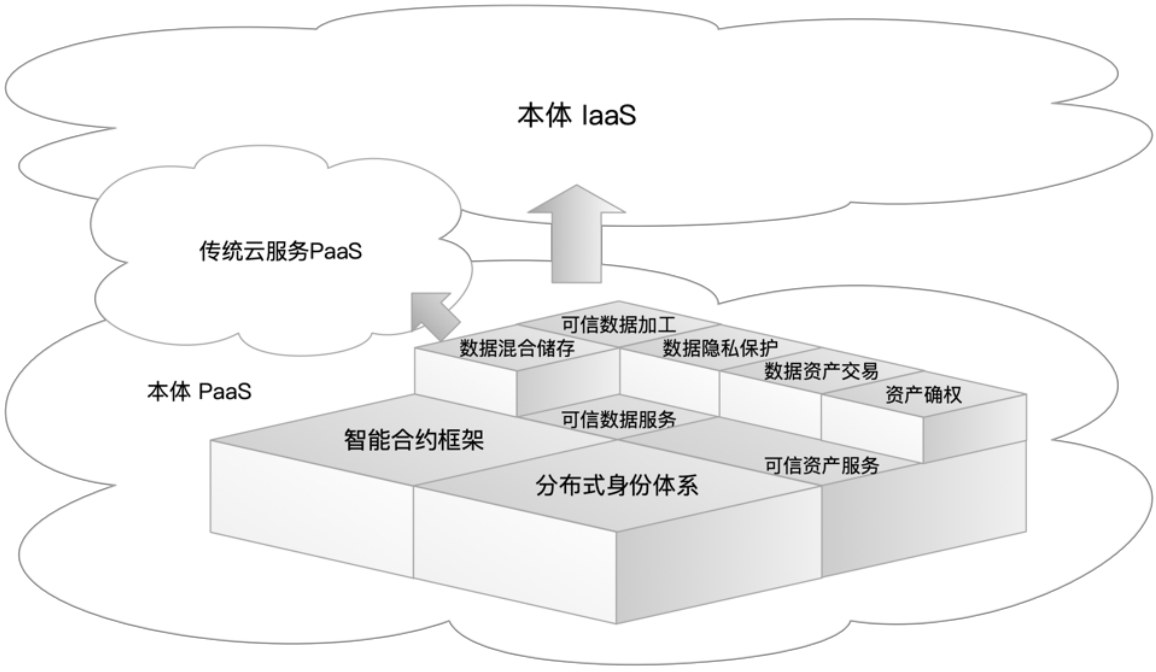


本体借助本体信任框架构建本体信任生态。本体区块链基础设施提供了防篡改和数据安全服务；本体数据交换框架提供可信数据服务，包含数据加工、隐私保护和安全数据储存的服务；本体标识协议针对数据确权和数据加工提供一致的实体标识和权限管理服务。

本体信任框架是本体实现分布式信任的核心逻辑层，我们通过分布式身份标识 ONT ID 来连接人、财、物、事，ONT ID 具有去中心化、自主管理、隐私保护和安全易用等特点。

在本体信任框架中，提出包括身份标识协议、多维实体认证协议用户授权协议和分布式数据交换协议等一系列的协议标准。各类协议的实现都兼容了国内外主要的协议标准和体系，如身份标识协议全面兼容 W3C 的 DID 方案；数字签名协议同时支持 ECDSA、SM2 和 RSA 等算法；在分布式数据交换体系中，兼容通用授权协议 OAuth、UMA 等，既使得架构具备开放性和标准性，亦可支持后续更广泛的生态合作与拓展。

本体会对应用服务做好“最后一公里”的支持，提供一系列应用框架，包括 API、SDK 以及各种应用功能组件，方便各行各业的应用服务提供方开发自己的 dApp。应用开发者无需具备底层的分布式系统开发能力，就可以直接基于本体提供分布式服务。



2. 术语说明

本体分布式账本

由本体的分布式账本/区块链框架构建的一个或多个核心公共服务基础链，为本体中的各项服务提供基础性的分布式账本和智能合约体系等服务。

分布式一致性账本

一种增量修改式的数据存储结构，由去中心化的点对点网络中的节点共同维护，具有数据公开且历史数据难以篡改的特点，为本体提供可信存储及智能合约支持。

智能合约

记录在账本中的可执行代码，通过账本节点上运行的智能合约引擎执行，每次执行的输入输出可记录在账本中。

实体

参与进行交互行为的个体，在本体中以 ONT ID 作为身份标识。

本体身份标识

ONT ID 是一个去中心化的分布式标识协议，用于本体上对人、财、物、事的身份关联，具有去中心化、自主管理、隐私保护和安全易用等特点。

可验证声明

一个实体对另一个实体（包括自己）的某些属性给出的描述性声明，并附加自己的数字签名，用以证明这些属性的真实性，可被其他实体验证。

分布式信任框架

本体实现分布式信任的核心逻辑层，主要包含分布式身份标识协议、分布式信任模型及分布式信任传递体系等部分。

多源认证

指多个不同的认证方从不同角度、不同方面对同一实体进行多维认证。

信任锚

被一定的实体群体所信任的实体，作为一些信任传递链的源头，为本体提供基础身份认证服务。

匿名声明

一种匿名的且不可连接的方式来出示用户的电子身份凭证。

身份认证

确认操作者身份的过程。常见的身份认证方式有口令、凭证和生物识别等。

非对称密码算法

也称公钥密码算法，即使用一对密钥的密码算法系统。密钥对包括一个可以公开的公钥和一个需要保密的私钥。

KYC

Know Your Customer。KYC 是一个业务流程，用于验证客户的身份并评估其适用性，以及识别业务关系中的潜在非法风险。

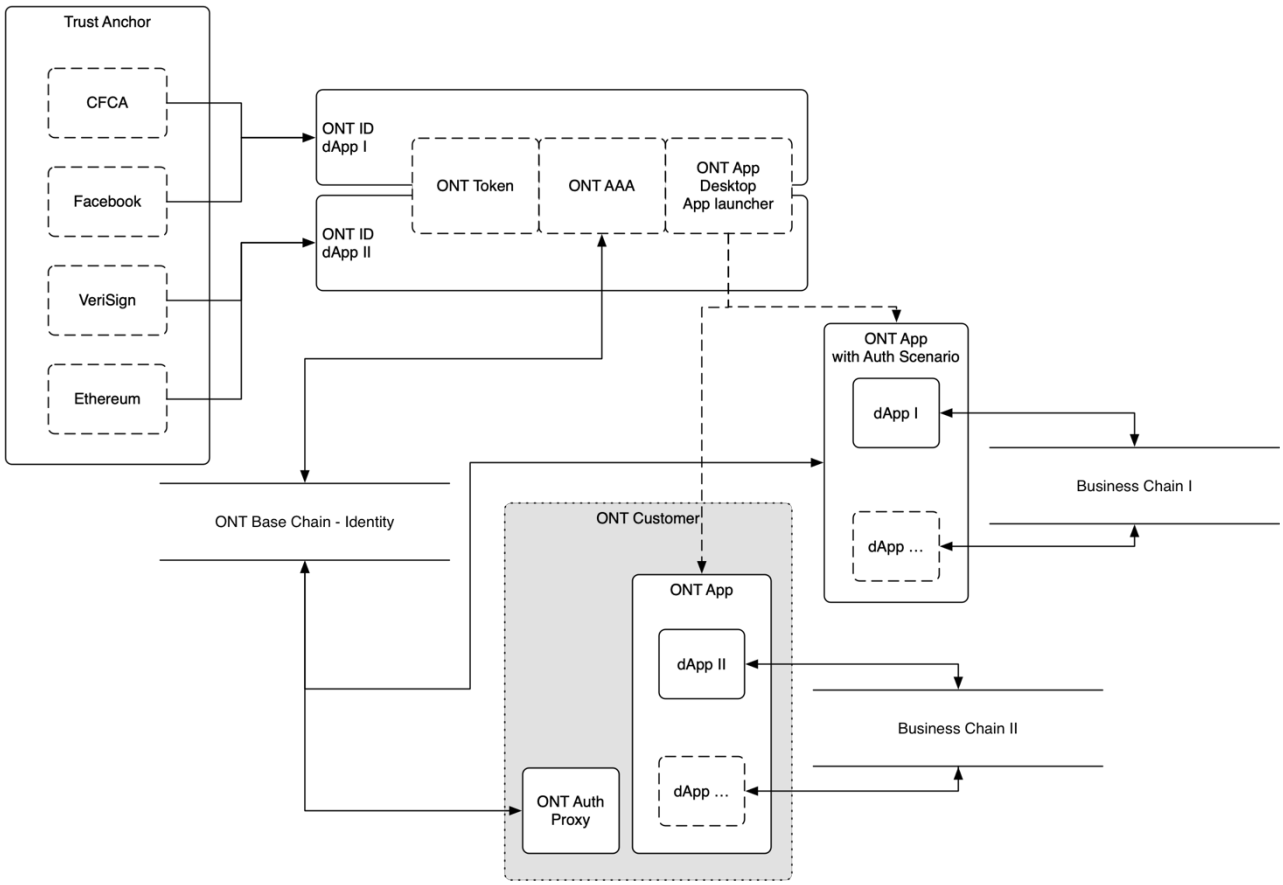
DID

分布式标识，是一种密码学中可验证和自管的标识。

3. 本体信任框架

本体区块链链网体系提供四个层次的服务，

1. 面向终端用户的可信应用体系；
2. 细分数据信息供求方，优化信息流转模式的可信信息传播体系方案；
3. 打通产业链上下游，构造良性竞争的商业诚信生态体系；
4. 地域合法合规，面向产业监管的可信仲裁体系。



图：本体 ONT ID 信任框架

本体信任框架的核心是：

1. 信任背书的设计，去中心化监督式竞争信任、分布式协同信任和中心化强信任锚点的多源信任体系；
2. 基于人、财、物、事的本体分布式实体标识（分布式本体标识）和可信声明体系设计；
3. 基于本体分布式标识，提供可信服务的功能链；
4. 满足不同业务的可信安全需求，平衡功能和性能的区块链服务框架。

在此基础之上，构建出基于信息资产的本体可信生态。

3.1. 本体标识协议

本体标识协议（ONT ID）定义了数据和数据所有者上链的过程、数据加工和所有权转移的过程。协议设计依照三个原则：

1. 支持三方系统账户体系的整合和上链，满足去中心化和用户自治的安全和隐私需求；
2. 支持数据加工过程和数据所有权转移，保证数据加工和所有权转移过程可追溯；
3. 支持数据所有权和数据加工权的解耦，保证数据加工和所有权转移的场景更加开放和灵活。

本体标识协议支持互联网服务，兼顾目前互联网和物联网的需求。考虑到区块链系统高价值的特性，本体标识协议需要支持高价值的数据服务。

综上，本体标识协议同时支持人、物、财、事的标识、记录和确权。

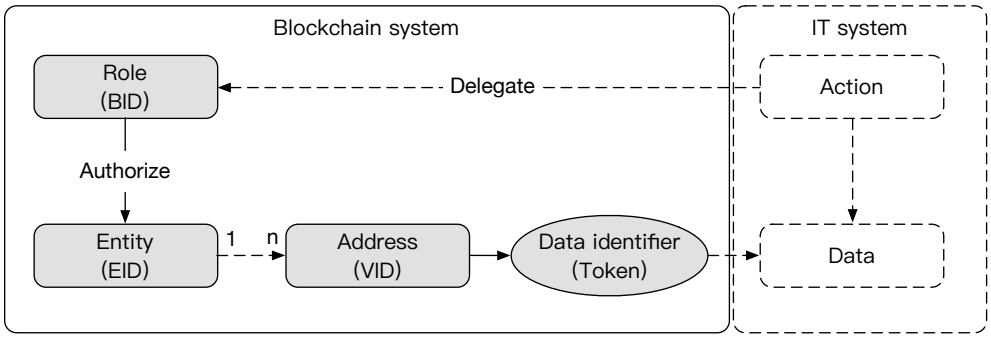
- 人和物的本质是“实体”。实体是指现实世界中的个人、组织（组织机构和企事业单位等）、物品（手机、汽车和 IoT 设备等）、内

容（文章和版权等），而身份是指实体在网络上的对应标识。本体使用本体身份标识（ONT ID）来标识和管理实体的网络身份。在本体上，一个实体可以对应到多个身份标识，且多个身份标识之间没有任何关联；

- 财的本质是数据信息的价值，通常以链上数字资产的方式定义，也可以指代数据本身，也可以成为一类“标识”；
- 事描述的是数据加工和所有权转移的过程。为了满足开放的应用场景，将数据所有者和数据加工者的角色进行解耦，引申出标识的另外两个层面，所有权标识和加工权标识。

本体标识协议包含实体标识、所有权标识和加工权标识，结合数字资产“标识”，形成本体信任框架的标识方案。其中，数字资产“标识”使用区块链“token”的设计。

本体标识方案如下图。



图：本体多层分片网络架构

定义：

- EID：实体标识；
- VID：数据所有者；
- BID：数据操作角色；
- Token：数据资产“标识”。

3.1.1. 自主管理

本体利用数字签名技术保障实体对自己身份标识的管理权。ONT ID 在注册时即与实体的公钥绑定，从而表明其所有权。对 ONT ID 的使用及其属性的修改需要提供所有者的数字签名。实体可以自主决定 ONT ID 的使用范围、设置 ONT ID 绑定的公钥，以及管理 ONT ID 的属性。

3.1.2. 多种公钥算法支持

本体支持多种标准化的数字签名算法，如 ECDSA、SM2 和 RSA 等。ONT ID 绑定的公钥需指定所使用的算法，同时一个 ONT ID 可以绑定多个不同的公钥以满足实体在不同的应用场景的使用需求。

3.1.3. 授权控制

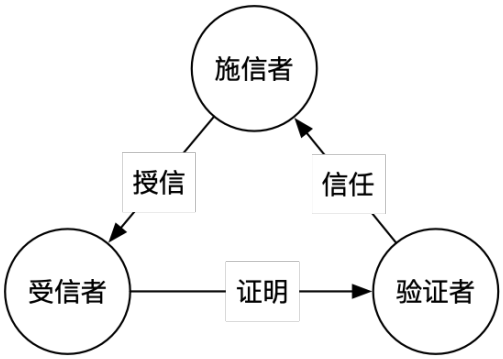
ONT ID 的所有者可以授权其他 ONT ID 代替本人行使对 ONT ID 的管理权，如修改 ONT ID 对应的属性信息，以预先授权的方式支持在密钥丢失时通过其它 ONT ID 绑定新公钥等。ONT ID 支持针对每条属性项的细粒度的权限管理，以及“与”、“或”、“m/n”等多种的访问控制策略。

3.2. 信任网络

本体信任网络是指本体生态中满足本体标识规范的实体之间形成的信任关系网络。本体信任网络由信任锚、可验证声明和多源认证协议组成。基于本体信任网络构建本体声誉体系。

3.2.1. 信任模型和信任锚

信任模型为信任场景提供支持，信任场景主要为受信者和验证者之间的业务合作构建信任渠道。信任模型由施信者、受信者和验证者三个角色组成，施信者为受信者背书，验证者通过信任施信者验证受信者。



图：信任模型

本体信任模型中，施信者被称为“信任锚”，含义为“验证者”通过“信任锚”来定位信任，以信任锚的信任凭证信任“受信者”。

此模型下，由一个或一群特定的实体作为信任锚，实体间的信任关系基于信任锚建立。信任锚指定其所信任的实体，被指定的实体又可指定其信任的其他实体。如此，以一个信任锚为源头，构建起一个信任传递的关系树。树上的每个节点有一条来自信任锚的路径，即为其信任链。任何承认该信任锚的实体在与树中的节点交互时，通过验证其信任链即可判断其是否可信。

信任模型是实体之间产生信任的机制，主要分为中心化的信任模型和去中心化的信任模型。本体同时支持这两种信任模型，可以根据具体场景选用不同信任模型适应不同需要。

3.2.1.1. 中心化的信任模型

目前应用最广的 PKI 体系就是一种中心化的信任模型。用户首先向作为信任锚的认证中心申请一个数字证书。认证中心对申请者审查通过后，将其身份信息和公钥写入数字证书，并附加认证中心的数字签名。通过认证中心签发的数字证书即认证了用户的身份和公钥的绑定关系，任何人都可以使用认证中心的公钥来验证该证书的真伪，进而使用证书中的公钥验证用户的签名，确认其身份。同时，拥有数字证书的用户还可以申请作为下级认证者对其它用户颁发数字证书，其颁发的数字证书的效力最终由认证中心保证。在 PKI 模型中，任何参

与方都必须无条件的信任认证中心，信任关系通过实体间的数字签名从认证中心逐层传递下去。

中心化的信任模型有很多优点，其严谨的信任传递方式、清晰明确的信任与非信任边界在很多场景下都是极佳的特性，解决了现实中的很多问题。然而，中心化的信任模式也存在一定的缺陷。除了需要无条件信任锚，对诚实性及安全性由较高的要求以外，面对现实世界的复杂信任关系，这种依赖于中心节点的模式会严重限制应用的灵活性。

3.2.1.2. 去中心化的信任模型

除了依赖特定的中心实体构建信任关系以外，实体之间还能够自发和对等地产生信任关系。信任的传递由实体间的相互认证实现。一个实体被数量越多的实体认证，其可信度就越高；被可信度越高的实体认证的实体，亦将获得更高的可信度。

去中心化的信任模型是一种支持多个信任源、多种信任维度的多元化信任，具有极高的灵活度。在不同的场景下可以根据不同的信任评估方法评估实体的信任度，这种高度的灵活性使其在现实生活中具有广泛的用途。

3.2.2. 可验证声明

可验证声明用来证明实体的某些属性。可验证声明可以作为一个数据单元进行存储和传输，并可被任何实体验证。可验证声明中主要包括声明元数据、声明事实及声明者的签名，其中声明事实可以是任意数据。

3.2.2.1. 生命周期

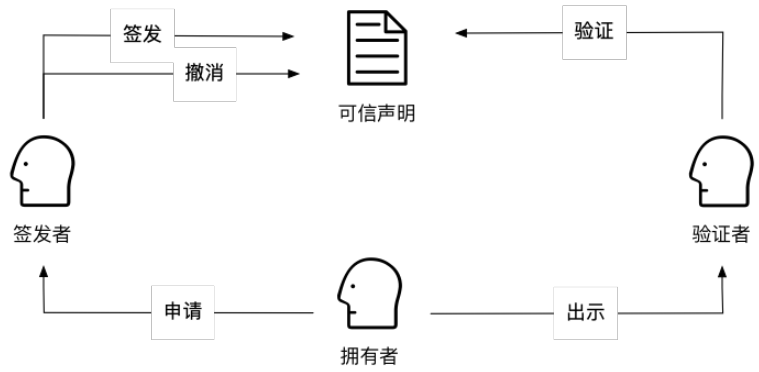


图 4.2 可验证声明的生命周期

与可验证声明相关的实体分为三种角色：施信者、受信者以及验证者。可验证声明的生命周期包括以下五种操作：

- 签发：任何实体都可以对其他实体的任何属性签发可验证声明，如学校可以给学生就一份成绩单签发一张可验证声明；银行可以就客户的资产状况签发一张可验证声明等。签发可验证声明时，可以设定声明的有效期，到期后声明自动作废。
- 存储：可验证声明可以分为公开声明和隐私声明。公开声明可以存储于本体的分布式账本中；隐私声明通常存储于实体的客户端中，由实体自己管理。
- 出示：受信者可以自主决定向谁公开声明，并且可以选择出示部分声明内容或者合并出示多张声明的部分内容而不影响对出示声明的验证。
- 验证：对可验证声明的验证不需要与声明的施信者交互，只需要根据施信者的 ONT ID 从本体的分布式账本中获取其公钥信息，进而使用该公钥验证声明中的数字签名，即可认证该声明的有效性。
- 撤销：可验证声明的施信者可以在声明有效期之前撤销声明，被撤销的声明将无法通过验证方的验证。

3.2.2.2. 匿名声明

通常情况下，受信者出示声明时会向验证者暴露声明的全部内容。在有些场景下，受信者希望既不向验证者暴露具体的声明内容，而又希望通过验证者的验证。针对于这种情况，本体使用匿名声明技术来保护用户的隐私。

匿名声明技术解决的问题，就是如何在签发及出示声明的过程中隐藏受信者的信息。利用匿名签发声明协议，同一个实体从两个不同施信者处获取两个声明，即使这两个施信者共谋也无法确认是否是将声明给了同一个实体。在匿名声明展示阶段，受信者不需要提供原始声明给验证者，仅需要提供一个零知识证明。验证者结合施信者的公钥和该证明，以及对证书中所包含属性值的一个断言（如 “年龄>18” 且 “持新加坡护照”），通过运行一个验证算法，可以验证声明的真伪。

一个匿名声明包含公开信息和密码学信息。公开信息包括匿名声明所涵括的所有属性，每个属性包括三个部分：属性名、属性类型和属性值。属性支持多种数据类型，如字符串、整数、日期和枚举类型。密码学信息主要包括受信者自己的主密钥，施信者对公开信息的数字签名。

在出示匿名声明的过程中，受信者向第三方验证者证明他拥有一张由某施信者签发的匿名声明，并且可以公开部分属性值而隐藏其它属性值。除此之外，还可以证明某些隐藏属性满足某些逻辑断言。

3.2.2.3. 可信执行环境

分布式账本的计算资源同样是有限且非常昂贵的，因此本体引入了可信执行环境（TEE）的解决方案，作为一个支持复杂算法的执行方案，将数据加工、数据互操作性和数据加工的高价值属性解耦，以可信执行环境支持复杂算法，以分布式账本服务提供数据加工的对账服务。

3.2.3. 多源认证协议

多源认证不同于以往的单一身份认证体系，本体为实体提供融合了外部信任源认证及本体中实体间背书的多源认证体系。多源认证协议包括以下两种模式：

- 外部信任源认证：本体外部信任源通过给自己签发可验证声明的形式绑定 ONT ID，以此加入本体信任网络。任何实体都可以通过验证 ONT ID 绑定的外部信任源来验证实体的身份。实体身份认证的可信度取决于 ONT ID 绑定的外部信任源的公信力；
- 本体实体间的身份认证：本体中的实体还可以通过本体中其它实体签发声明的方式实现身份认证。

3.2.3.1. 外部信任源认证

外部信任源认证支持自我导入和信任锚导入两种方式。

1. 自我导入

用户通过社交媒体、银行 UKEY 签名等方法来绑定现实信任，该模式利用了现实世界已有的信任，通过在本体上添加一个外部信任源的证明地址，并且在该证明地址上提供一个可验证声明实现。内容包括：

- 声明创建与过期时间；
- 声明内容：包含声明的类型、ONT ID、社交媒体类型和社交媒体的用户名等；
- 签名：需要指定使用的公钥，必须是 ONT ID 描述信息中公钥列表中的一个。

当第三方需要验证用户的外部身份时，首先在本体中读取到用户信任源的证明地址，然后到这个地址去获取可验证声明，最后验证该可验证声明即可。

2. 信任锚导入

信任锚遵守本体相关标准，由验证者信任的施信者实体组成。信任锚使用自有的认证方式对受信者进行认证后，对受信者签发一个可验证声明。声明中不需要包含受信者的真实身份信息，仅记录实体及认证服务的 ONT ID，作为该服务的认证结果证明即可。其认证模型如下：

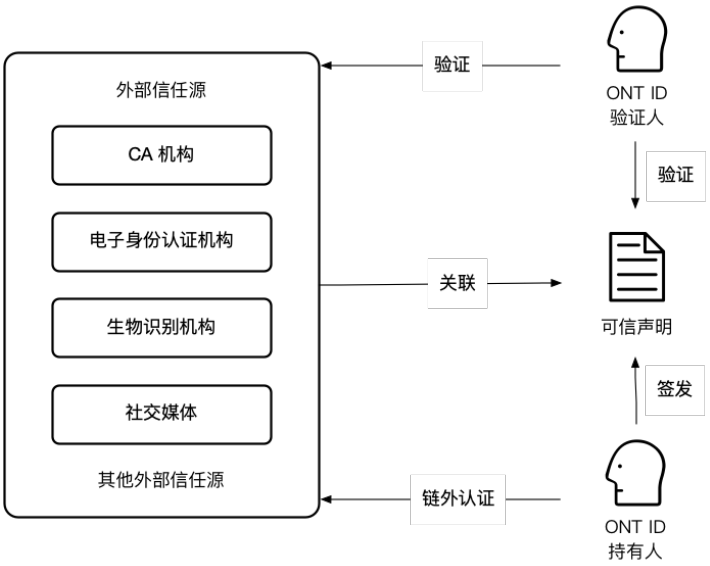


图 6.1 外部信任锚认证

3.2.3.2. 本体实体间的身份认证

本体中的实体可以通过本体中已通过施信的受信实体来实现间接施信。如图 6.2 所示，用户不仅可以通过学校和银行等实体做身份认证，还可以通过个人等其他方式获得身份认证。

正是由于可验证声明的开放性，使得本体中任何实体可以对任何另一实体就任何事情发布声明，这使得本体中的身份认证远远超过传统的身份认证概念。这种多角度、多方面的认证相比传统的单一认证更准确与全面。

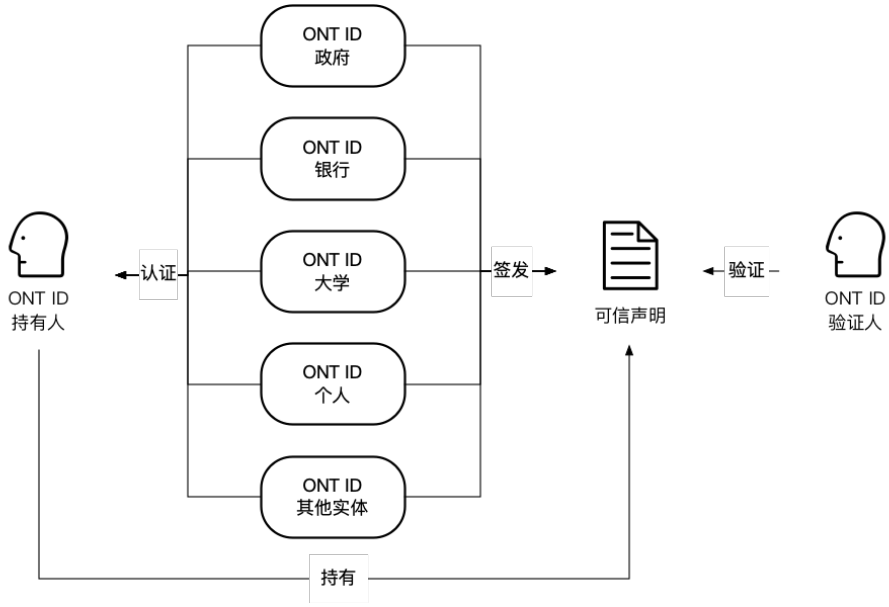


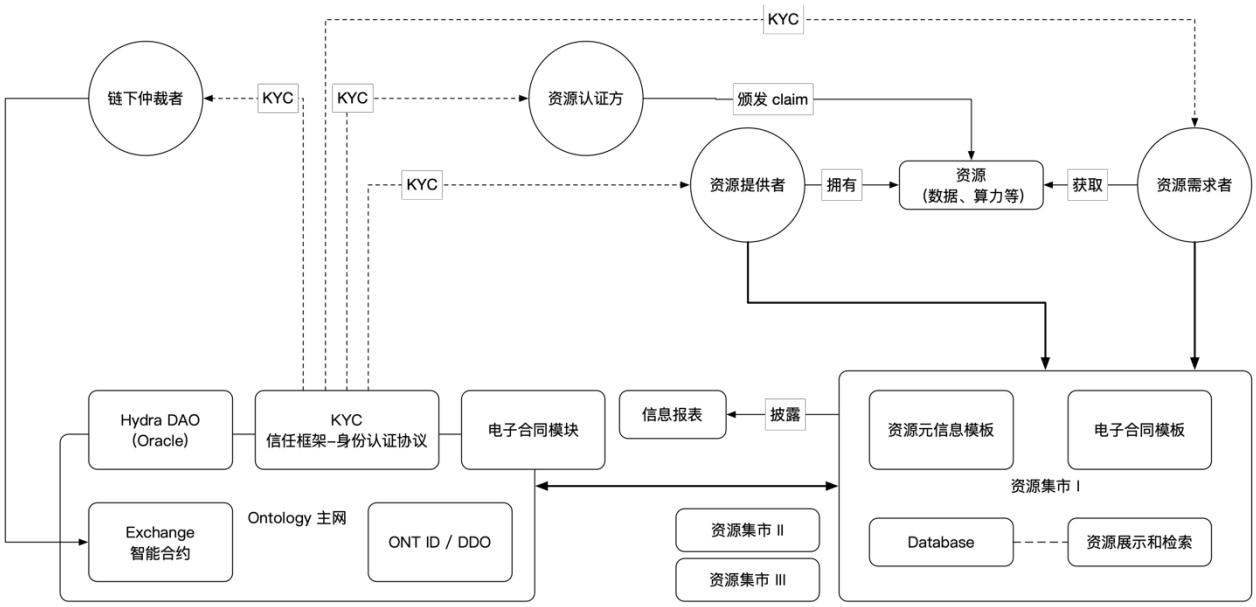
图 6.2 实体间身份认证

3.2.4. 分布式声誉体系

分布式声誉体系是本体信任网络的重要组成部分，将本体信任网络和本体业务应用结合起来。一方面，通过受信者声誉评价为应用验证者导流，提升应用对于用户交互体验的设计，更好地服务用户；另一方面，用户使用不同的业务应用，应用作为施信者为受信者用户提供信任背书，良好的声誉可以帮助用户得到更多更好的服务，受信者通过持续的积累本体生态中的声誉，促进整个生态应用的用户质量良性发展。

4. 分布式数据交换框架

分布式数据交换框架（DDXF）通过一致性账本、智能合约和密码学等技术实现实体资源和链上资产的去中心化交互、分享、交换与协作。



图：DDXF 框架

基于 DDXF，可以实现资源链上确权和流转平台，可以以资源交换 ONG、OEP-4 等数字资产，或者以资源交换资源。DDXF 支持的资源包括数字资源和实体资源。DDXF 支持的资源流转形式包括数字资源流转和实体资源流转。资源的链上流转包含资源的所有权、使用权或者其它相应权利的流转。对于链下实体的资源，DDXF 支持链下交割，通过电子合同等方式的设计，兼顾链下行为的合规性，同时保证链上链下行为的安全性和一致性。

4.1. 本体资源资产化

资源资产化是指把链外资源数字化、标准化之后，将资源和本体身份体系进行链上绑定，获得资源的 ONT ID，将资源的相应权利 Token 化，由此完成资源资产化的全过程。DDXF 使用资源 Token 进行链上协作和交换。

根据资源相应权利的特性进行 Token 的创建、销毁和分发，对应同质化 Token、非同质化 Token 和半同质化 Token。结合 ONT ID 业务操作权限管理的方案，支持对资源权利转移的过程进行追溯。

Token 可以交易，在资源资产化基础之上，本体方案包含对资源的元信息进行描述，以此参与 Token 价值量化和交易。

本体采用 DToken 协议实现资源资产化。DToken 是由一系列不同功能的协议组成，包含资源元信息抽取、元信息模板定义、资源 Token 化标准、DToken 价值绑定、DToken 权利转移协议等。在实际使用过程中，针对业务的使用场景，业务可以自由选择自己合用的模块进行业务封装。

4.2. 分布式数据交换协议

本体提出分布式数据交换协议，并将应用场景推广到所有有价值的资源。针对目前中心化数据交易所的痛点如：数据缓存、隐私数据未经用户授权和数据版权无法保护等问题。分布式数据交换协议对实体之间的数据交互行为定义了一整套协议规范。

为了保证交互过程的安全性和交互参与方的权益，分布式数据交换协议定义了通用的交互场景，细化了交互过程中的角色并对角色的行为进行了规约并在架构上做了开放性接口的设计，保证链下资源和链上资产交互、分享和交换过程的一致性和安全性。

4.2.1. 角色定义

在分布式数据交换协议中主要的角色有：

- 资源提供者(RP)。拥有资源的实体，并将资源开放给市场，以资源通过某种定价体系获取一定的收益。此类实体有很多种类，比如数据所有者、算力拥有者、数据收集平台以及具有一定权限的数据托管方等；
- 资源需求者(RC)。资源提供者的交易对手方，是需要某种资源的实体，从资源提供者中获取资源的（部分)权利，并为此支付一定的费用；
- 资源认证方(RA)。具有一定权威性的第三方，以拥有自己的资源质量认证体系，根据该体系可以给资源或者资源提供者提供一定方式的认证以增强资源或者资源提供者的可信度；
- 链下仲裁者(OJ)。资源提供者和资源需求者在资源交易中都认可的链下纠纷仲裁者。链下产生的纠纷将由链下仲裁者进行裁定；
- 交易市场(MP)。联系资源提供者和资源需求者的纽带，存储资源的元信息，为资源提供灵活的展示和快捷的搜索，收取交易费用。每个交易市场可以按照自身交易的特性提供伸缩化的灵活服务，比如提供元信息模板、解决链下纠纷的电子合同模板等供交易双方具现化使用。交易市场拥有资源交易定价体系，也拥有资源交易信息披露体系，可以对公众或者监管部门进行交易信息披露。

4.2.2. 用户授权机制

数据交换体系中，由于交易的数据需要通过资源所有者的授权，授权流程完全遵守用户授权协议，其协议定义参考用户授权协议。

4.2.3. 数据交换流程

1. 资源准备:

    a. (可选)RP 从 RA 处取得对准备发布资源的认证;

    b. RP 针对将要发布的资源在链上生成一个 ONT ID 以及相应的信息，作为资源在链上的映射;

    c. 根据 MP 提供的定价体系，确定具体的定价方式;

d. 根据 MP 提供的资源元信息模板生成相应的资源元信息;

2. 资源发布:

   a. RP 提交资源 ONT ID、元信息以及定价方式等给 MP;

   b. MP 从链上以及自身数据库等处获取该资源对应的信息;

   c. MP 做资源展示，使得 RC 能根据资源元信息等快速检索相应资源;

3. 资源交易:

   a. RC 在 MP 处根据资源元信息等快速检索到所需资源，确定想要交易的资源;

   b. RP 和 RC 根据 MP 的电子合同模板具现化双方交易的电子合同，指定 OJ，并经由电子合同进行签名，并在交易智能合约中进行记录。根据 MP 或者合同要求，RP 和 RC 可能需要分别向交易智能合约质押一定量的 ONG，用做纠纷处理和交易后分润;

   c. RP 根据电子合同生成 D Token，将资源的某项权利，例如(部分)所有权或者使用权，授权给 RC;

   d. 交易进入锁定期，RP 将使用 D Token 来换取对资源相应的处置权利;如果在交易锁定期中产生纠纷，双方提交链上证据或者链下证据。链下证据由 OJ 或者 HydraDAO 将介入并进行裁定;

4. 分润:

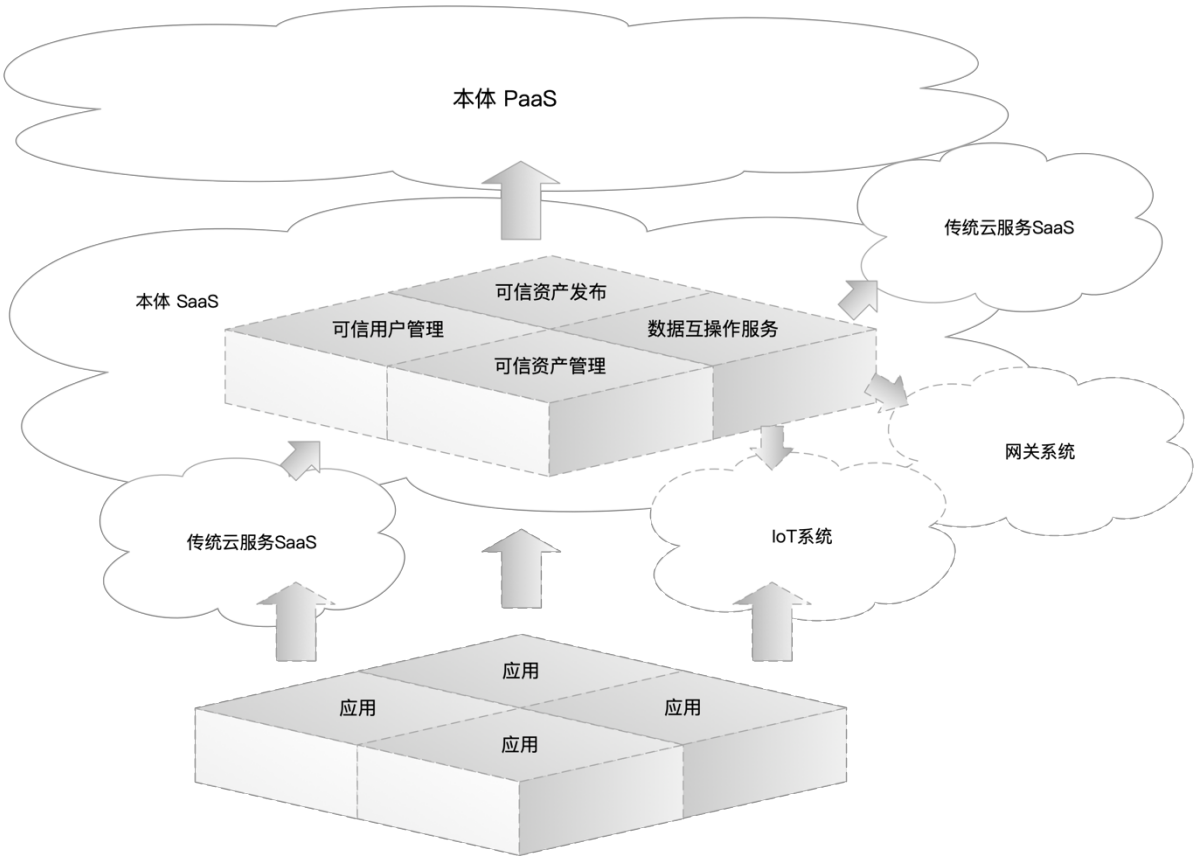
   a. 在锁定期结束后，根据交易结果进行分润。OJ 或者 HydraDAO 对纠纷的判定可能提前触发分润;

5. 交易后评价:

   a. RP 和 RC 进行双方互相评价，评价可以针对资源或者用户;

5. 本体应用框架

基于本体信任框架和本体分布式数据交换框架，提出本体应用框架。



图：本体应用框架

本体应用框架提供了一系列丰富的应用层协议和组件，帮助应用开发者快速构建出去中心化应用，使其不用花精力关注底层分布式账本交互的复杂性。本体应用框架具有高度的可扩展性，可以根据实际场景的需要，不断进行扩展。

图 7.1 为应用框架模型示意。dApp 通过应用框架与本体交互，实现去中心化信任。

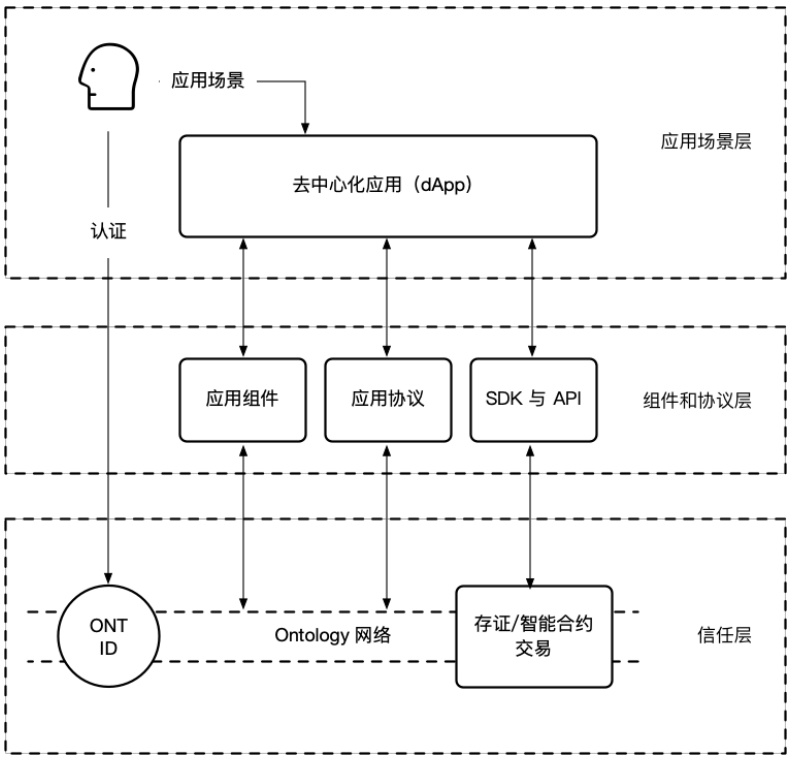


图 7.1 应用框架模型示意图

本体通过去中心化的身份体系、存证和智能合约交易等技术实现了分布式信任；通过应用组件、应用协议、SDK 和 API 帮助上层场景更好地使用本体。业务 dApp 关注业务场景开发和用户服务等。

5.1. 本体应用接入

基于本体的应用框架，本体为应用接入提供可信资产发布、可信用户管理、可信资产管理和数据互操作服务。本体生态伙伴可以就这四个模块进行二次封装，形成解决方案，为本体应用生态提供服务。

本体提供可信应用解决方案，支持业务应用接入本体可信生态。可信业务应用形成应用市场，支持终端用户自行选择业务应用。同类业务在可信生态中良性竞争，推进业务发展，形成应用市场。本体生态的分布式声誉体系是应用市场的一个必要组件。

6. 后记

本书描述本体信任框架采用的技术和协议，将随着更多应用的拓展而持续更新。

本体努力打造一个开放、协作和创新的生态，诚挚欢迎您加入我们，共同参与和推进本体项目。

联系我们

电子邮件：
contact@ont.io

Telegram：
OntologyNetworkCN

Twitter：
OntologyNetwork

Facebook：
ONTnetwork

Reddit：
OntologyNetwork

Discord：
https://discord.gg/vKRdcct

Medium：
OntologyNetwork

LinkedIn：
Ontology

微信公众号：
本体 Ontology

微信客服：
本体研究院小秘书